Reference 1
Japanese Patent Disclosure No. 2000-224156

(43)Date of Disclosure: August 11, 2000
(21)Japanese Patent Application No. 2000-12643
(22)Filing Date: January 21, 2000
(31)Convention Priority Number: 99101457.2
(32)Date of Priority: January 27, 1999
(33)Country of Priority: EPO

(71)Applicant: International Business Machines Corporation
(72)Inventor: Hermann Reto

The above Japanese Patent Disclosure No. 2000-224156 corresponds to European Patent Application No. 99101457.2.
The paragraphs in JP Publication to which the Examiner notices correspond to those paragraphs in EP publication as follows.

JP Publication	EP publication
0010	0011
0041	0044
0051	0054

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－224156
（P2000－224156A）
(43)公開日　平成12年８月11日(2000.8.11)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ	9/00	６０１Ｄ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｅ
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ	7/26	１０９Ｍ
Ｈ０４Ｌ　12/28				１０９Ｓ
		Ｈ０４Ｌ	9/00	６０１Ｆ

審査請求　有　　請求項の数27　ＯＬ　（全 11 頁）　　最終頁に続く

(21)出願番号　特願2000－12643(P2000－12643)

(22)出願日　平成12年１月21日(2000.1.21)

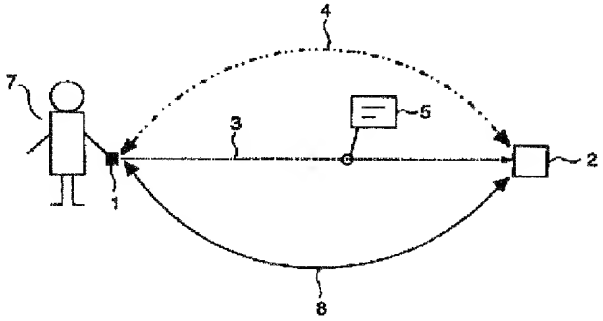
(31)優先権主張番号　９９１０１４５７．２
(32)優先日　平成11年１月27日(1999.1.27)
(33)優先権主張国　欧州特許庁（ＥＰ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）
(72)発明者　レト・ハーマン
スイス、シィ・エイチ－8863　ブッティコン、プールストラッセ　5
(74)代理人　100086243
弁理士　坂口　博　（外１名）

最終頁に続く

(54)【発明の名称】　ネットワーク化普及環境における情報交換のための方法、装置及び通信システム

(57)【要約】
【課題】　ネットワーク化普及環境における情報交換のための方法、装置及び通信システムを提供すること。
【解決手段】　認証された及び秘密のセッションが達成される。従って、第１の装置及び少なくとも第２のリモート装置が使用される。第１の装置及び第２のリモート装置間の単方向無線通信チャネルが始動され、第１の装置から第２のリモート装置への単方向無線通信チャネルを介して、シーケンスが送信され、第２のリモート装置に暗号化情報を提供する。前記暗号化情報を暗号化のために使用することにより、暗号化応答が無線同報媒体を介して第１の装置に送信される。



1

【特許請求の範囲】

【請求項１】第１の装置と少なくとも第２のリモート装置との間の情報交換のための方法であって、

前記第１の装置と前記第２のリモート装置との間の単方向無線通信チャネルを始動するステップと、

前記単方向無線通信チャネルを介して、前記第１の装置から前記第２のリモート装置にシーケンスを送信し、前記第２のリモート装置に暗号化情報を提供するステップと、

前記暗号化情報を暗号化のために使用し、無線同報媒体を介して、前記第１の装置に暗号化応答を送信するステップとを含む、方法。

【請求項２】前記２つの装置が前記無線同報媒体を共用し、ローカル・ネットワークの一部である、請求項１記載の方法。

【請求項３】前記単方向無線通信チャネルが光チャネル、パーソナル・エリア・ネットワーク（ＰＡＮ）・チャネル、有向無線周波チャネル、誘導性チャネル、または容量性チャネルである、請求項１記載の方法。

【請求項４】前記単方向無線通信チャネルが有向チャネルである、請求項１または請求項３記載の方法。

【請求項５】前記有向単方向無線通信チャネルが視線リンクである、請求項４記載の方法。

【請求項６】前記第１の装置の初期送信機が、前記単方向無線通信チャネルが前記第２の装置に向けられるように配置される、請求項１記載の方法。

【請求項７】前記無線同報媒体が光チャネル、音響チャネル、無線周波（ＲＦ）チャネル、ホームＲＦチャネル、ブルートゥース・チャネル、またはパーソナル・エリア・ネットワーク（ＰＡＮ）・チャネルである、請求項１または請求項２記載の方法。

【請求項８】前記単方向無線通信チャネルが数メートルの通達距離を有し、前記無線同報媒体のチャネルが、前記単方向無線通信チャネルの前記通達距離と同一の、またはそれ以上の通達距離を有する、請求項１記載の方法。

【請求項９】前記第２のリモート装置が前記シーケンスを受信する、請求項１記載の方法。

【請求項１０】前記第２のリモート装置が前記第１の装置からの前記シーケンスの受信を、光または音響信号により知らせる、請求項１記載の方法。

【請求項１１】前記第２のリモート装置が前記シーケンスを周期的に傾聴する、請求項１記載の方法。

【請求項１２】前記第１の装置がユーザに接続され、前記ユーザが前記第２のリモート装置に触れることにより、該ユーザの人体を介して前記単方向無線通信チャネルを始動する、請求項１記載の方法。

【請求項１３】前記２つの装置の１つが、少なくとも通信パラメータまたはセッション・キーを送信する、請求項１記載の方法。

2

【請求項１４】前記無線同報媒体を介する前記応答が、公開キー暗号化システムを含む、暗号化システムにより保護される、請求項１記載の方法。

【請求項１５】前記暗号化情報がパスワードまたは公開キーを含む、請求項１記載の方法。

【請求項１６】少なくとも１つのリモート装置との情報交換のための装置であって、

単方向無線通信チャネルを介して、前記リモート装置にシーケンスを送信する初期送信機と、

前記リモート装置から無線同報媒体を介して暗号化情報を受信する受信機と、

前記単方向無線通信チャネルを介して前記リモート装置に送信可能な暗号化情報を提供する暗号化システムとを含み、

前記受信機が前記無線同報媒体を介して、前記暗号化システムにより処理可能な暗号化情報を受信する、装置。

【請求項１７】少なくとも１つの装置との情報交換のための装置であって、

単方向無線通信チャネルを介して、前記装置からシーケンスを受信し、暗号化情報を獲得する初期受信機と、

前記暗号化情報を処理する暗号化システムと、

暗号化情報を無線同報媒体を介して前記装置に送信する送信機とを含む、装置。

【請求項１８】情報を符号化及び復号する暗号化システムを有する第１の装置及び第２の装置を含む、情報の交換のための通信システムであって、

前記第１の装置が、

単方向無線通信チャネルを介して、前記第２の装置にシーケンスを送信し、前記第２の装置に暗号化情報を提供する初期送信機と、

無線同報媒体を介する前記第１及び第２の装置間の暗号化通信のための第１のトランシーバとを含み、

前記第２の装置が、

前記単方向無線通信チャネルを介して、前記第１の装置から前記シーケンスを受信し、前記暗号化情報を獲得する初期受信機と、

前記無線同報媒体を介する前記第１及び第２の装置間の暗号化通信のための第２のトランシーバとを含む、通信システム。

【請求項１９】前記無線同報媒体を介して暗号化情報を送信可能な送信機を含む、請求項１６記載の装置。

【請求項２０】前記初期送信機が前記シーケンスを前記単方向無線通信チャネルを介して、数メートルの通達距離内で送信する、請求項１６記載の装置。

【請求項２１】前記無線同報媒体が光チャネル、音響チャネル、無線周波（ＲＦ）チャネル、ホームＲＦチャネル、ブルートゥース・チャネル、またはパーソナル・エリア・ネットワーク（ＰＡＮ）・チャネルである、請求項１６または請求項１７記載の装置。

【請求項２２】前記無線同報媒体が前記単方向無線通信

チャネルの通達距離と同一の、またはそれ以上の通達距離を有する、請求項１６または請求項１７記載の装置。

【請求項２３】ＬＥＤなどの光装置またはラウドスピーカなどの音響装置により、前記シーケンスの受信を知らせるシグナル装置を含む、請求項１７記載の装置。

【請求項２４】前記初期受信機が前記シーケンスを周期的に傾聴する、請求項１７記載の装置。

【請求項２５】前記２つの装置の１つが通信パラメータ及びセッション・キーを送信できる、請求項１８記載の通信システム。

【請求項２６】前記２つの装置が前記無線同報媒体を共用し、ローカル・ネットワークの一部である、請求項１８記載の通信システム。

【請求項２７】前記第１の装置の前記初期送信機が、前記単方向無線通信チャネルが視線リンクにより前記第２の装置に向けられるように配置される、請求項１８記載の通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワーク化普及環境における情報交換のための方法、装置及び通信システムに関し、特に、装置が認証されたセッションまたは秘密セッションに参加することを可能にする初期技法に関する。

【０００２】

【従来の技術】コンピュータは、劇的に小型化され、携帯可能となった大規模で珍しい孤立した装置である。パーソナル・コンピュータ及び周辺装置は、机上に載置可能なように十分に小さくなった。より小型のものにラップトップ・コンピュータ及びノートブック・コンピュータがある。配送トラックなどの乗り物に搭載可能なように、十分に小さなコンピュータ端末が存在する。更に小型のものにハンドヘルド端末があり、これは一般にその携帯性により、ユーザが片手で端末を持ち運び、もう一方の手でそれを操作することができる。ケーブルまたはファイバによる前記装置の物理接続はケーブルの長さ制限や、コンピュータ上のポート数の制限、従って接続可能な周辺装置の数の制限、或いはハードワイヤード装置の厄介な再構成などのために構成的制限などの欠点を有する。コンピュータ上の限られたポート数が、実際には周辺装置の数を制限しない幾つかの周辺インタフェース・システムが存在する。ユニバーサル・シリアル・バス（ＵＳＢ）及びＩＥＥＥ１３９４（ファイヤワイヤ）は、単一ポート上で非常に多数の装置をサポートできる周辺バス・システムの例である。イーサネットは、ケーブルが共用媒体として使用される通信システムの例である（他の例にはトークン・リング、ＦＤＤＩ（ファイバ分散データ・インタフェース）、及びＤＱＤＢ（分散キュー・デュアル・バス）がある）。

【０００３】装置が小型化するほど、固定の物理接続を無線アドホック接続（例えば人体ネットワーク、無線周波接続、または赤外線接続）により置換することが重要となる。なぜなら、コンピュータ端末、周辺装置、及び他の装置をケーブルまたはファイバにより物理的に接続することは、ユニットを小型化することにより得られる効果を多大に低減するからである。装置が移動され、ある領域から出たり入ったりする場合、アドホック接続が要求される。用語"アドホック（ad-hoc）"は頻繁なネットワーク再構成の必要性を指す。

【０００４】ローカル・エリア通信は、パーソナル・ローカル・エリア・ネットワークと呼ばれるものに急速に発展しつつある。これはローカル・ピアまたはサブシステム間の通信のためのネットワークである。これらの種類のネットワークを、ここではローカル・ネットワークと呼ぶことにする。無線通信はこうしたローカル・ネットワークでは、特に重要である。こうしたローカル・ネットワークのピアまたはサブシステム間の通信を目的とする、既知の異なる無線通信アプローチが存在する。

【０００５】ローカル・ネットワークの典型的な例は、パーソナル・エリア・ネットワーク（ＰＡＮ）であり、これはマサチューセッツ工科大学（ＭＩＴ）メディア研究所の２つの研究グループ間の業績により誕生した。人体の自然塩分は、人体を電流の優れた導体にする。ＰＡＮ技術はこの導電性を利用する。ＰＡＮ技術はごく僅かな電流を用いて、ユーザの識別及び他の情報をある人から別の人に、或いは自動車、公衆電話、自動預金支払機（ＡＴＭ）などの様々な日常物にさえも伝送する。情報は、厚いクレジットカード・サイズのＰＡＮ送信機及び受信機内に配置されるマイクロプロセッサを介して転送される。次にデジタル・データが、微小の外部電界を介して送信または受信される。小信号が人体の自然塩分により伝導され、気付かれることなく、情報を人体を通じて伝達する。低周波及び低電力の信号は個人に符号化される情報が人体を超えて伝達されず、人体と接触するある物または誰かによってのみ受信されることを保証する。情報が現在伝送されるスピードは、２４００ボー・モデムに等価である。理論的には、この方法により４００００００（すなわち４００ｋ）ビット／秒が伝達され得る。ＰＡＮは固定のケーブル接続などを要求しないアドホック人体ネットワークの典型的な例である。

【０００６】ＰＡＮ技術はビジネス、医療、小売り、及び個人分野においてさえ、潜在的なアプリケーションを有する。例えばビジネス仲間は握手を交わしながら電子名刺を交換する。企業の機密装置は、自動的にユーザをコンピュータ・システムにログオン及びログオフし、地下鉄通勤者は回転式改札を通過することにより、乗車運賃を支払う。ＰＡＮ技術により、人々は自身の医療ファイルのデジタル・バージョンを持ち運び、それにより緊急医師による即時アクセスが可能となる。或いは、呼び出しカード番号が自動的に財布から公衆電話に送信され

得る。また、ＡＴＭ及び自動車はそれらの所有者が近づくとき、即時所有者を識別することができる。別のアプリケーション分野は、売買に参加するために立合場で素早く且つ確実なログオン及びログオフを要求する商人に当てはまる。ＣＤプレーヤ、テレビ及びトースタなどの家電機器でさえも、ＰＡＮ技術の使用により、個人の嗜好及び味覚を識別し、それらに適応することができる。ＰＡＮネットワークは通常ポイント間通信であり、そこでは人体が同報通信媒体として作用する。

【０００７】ＧＴＥ社は、セルラ電話、ページャ、及びハンドヘルド・パーソナル・コンピュータ（ＰＣ）などの移動装置をターゲットとする、お互いの対話にとって好適な短距離無線周波（ＲＦ）技術を開発した。ＧＴＥ社の技術は暫定的に、ボディＬＡＮ（ローカル・エリア・ネットワーク）と命名される。ボディＬＡＮの元々の開発は、様々な装置に接続された配線付きベストを介するものであった（これがボディＬＡＮの名前に由来する）。これが数年前にＲＦ接続へと進歩した。

【０００８】ゼロックス社は、ＰＡＲＣ　ＴＡＢと呼ばれるハンドヘルド・コンピュータ装置を開発した。ＰＡＲＣ　ＴＡＢは携帯式であるが、既知のロケーションを有するベース・ステーションを介して、オフィス・ワークステーションに接続される。ＰＡＲＣ　ＴＡＢベース・ステーションは建物のあちこちに配置され、固定の配線式ネットワークに配線される。ＰＡＲＣ　ＴＡＢシステムは、建物レイアウトの所定の知識、及び様々なベース・ステーションの識別子を用いることにより、最も強いベース・ステーション信号により、自身がどこにあるかを決定する。ＰＡＲＣ　ＴＡＢシステムは、ＰＡＲＣ　ＴＡＢ携帯装置が常にネットワーク構造基盤に接続されているものと仮定する。各ＰＡＲＣ　ＴＡＢ装置のロケーションは、常にシステム・ソフトウェアに知れている。ベース・ステーションは領域を確立し、電源に接続される。ＰＡＲＣ　ＴＡＢ通信システムはスター型トポロジを有する。

【０００９】異種のＰＣ装置間のデータ通信を標準化するために、エリクソン、ＩＢＭ、インテル、ノキア（Nokia）及び東芝を含む幾つかの会社が、固定の携帯用移動装置間の無線ＲＦベースの接続のための世界標準を作成するために、ブルートゥース（Bluetooth）・コンソーシアムを確立した。多くの他の採用会社が存在する。提案された規格は、物理層からアプリケーション層までのアーキテクチャ及びプロトコル仕様を含む。この技術は例えば、ユーザがオフィスに入るとき、移動装置内に保持されるアプリケーション情報を、固定のデスクトップ・コンピュータ内に保持される同様の情報と自動的に同期させる解決策を可能にする。ワイヤレス短距離無線を介して、継ぎ目の無い音声及びデータ伝送を可能にすることにより、ブルートゥース技術はケーブルを必要とすることなく、ユーザが様々な装置を容易に且つ迅速に接続することを可能にし、移動コンピュータ、移動電話及び他の移動装置の通信能力を拡大する。ブルートゥース動作環境はまだ完全に定義されていないが、ＩｒＤＡ（赤外線データ・アソシエーション）仕様及び拡張赤外線（ＡＩｒ）仕様との類似点があるものと期待される。多分ブルートゥースに盛り込まれるであろう他の態様は、ＩＥＥＥ規格８０２．１１、及び欧州電気通信規格協会（ＥＴＳＩ）により公布されたＨＩＰＥＲＬＡＮに由来するであろう。

【００１０】ブルートゥース無線技術は、固定のネットワーク構造基盤から離れて存在する接続装置の、小規模で専用のアドホックグループを形成する機構を提供する。ブルートゥースは、マスタ・ユニットと、同一のネットワーク・セグメント内のスレーブ・ユニットとを区別し、前者はそのクロック及びホッピング・シーケンスが、他の全ての装置を同期するために使用される装置である。換言すると、ブルートゥース・アプローチは集中化される。照会ベースの発見技法が、未知のアドレスを有するブルートゥース装置を見いだすために使用される。照会はまた、レジストリ・サーバにおいて集中化される。故障の中央ポイントが存在することは、こうした集中型アプローチの欠点である。こうしたシステムの別の欠点は、分散技法よりも多くのオーバヘッドが要求されることである。こうしたシステムの主問題は、単一のレジストリ・サーバを突き止めることにあり、それが消えた場合にどうすべきかにある。無作為の２つの装置が互いに遭遇する場合、それらは最初にお互いの存在を認識し、次にどちらがレジストリ・サーバかを決定し、続いてそれらの通信の作業に取りかからねばならない。オーバヘッドの増加を生じるのは、リーダのこの頻繁な選択及び再選択である。別の方法は、ユーザが常にある装置を身につけて持ち運んでいるものと期待し、それを常にリーダとすることである。しかしながら、これは常に現実的な選択とは限らない。

【００１１】ＩｒＤＡは、赤外線技術の品質及び相互運用性を保証する赤外線規格及び仕様を提供することを目的とする、世界中の１５０社以上の協会である。ＩｒＤＡ－Ｄは、１ｍの距離のデータ転送用に設計された赤外線データ伝送規格であり、１１５ｋビット／秒乃至４Ｍビット／秒、または近い将来１６Ｍビット／秒をサポートする予定である。広範囲のハードウェア及びソフトウェア・プラットフォームがサポートされる。ＩｒＤＡデータは、相互運用可能な汎用双方向コードレス赤外線光伝送データ・ポートのための規格を定義し、高速短距離、視線、ポイント間コードレス・データ転送に適している。ＩｒＤＡデータ・プロトコルは、強制プロトコルと任意プロトコルのセットを含む。しかしながら、元来の仕様は幾つかの欠点を示し、ある時点に１対の装置だけが同一の赤外線空間において通信可能なように、データ通信を制限する。ヒューレット・パッカード及びＩＢ

Mの両者間の協力により、次世代の赤外線データ通信システムを定義する拡張赤外線（ＡＩｒ）と呼ばれる別の仕様が開発された。ＡＩｒは、室内におけるマルチポイント対マルチポイント接続のために提案される。距離及びデータ速度は可変であり、８mの距離において２５０ｋビット／秒から、４mの距離において４Mビット／秒の範囲に及ぶ。これは複数の周辺装置へのコードレス接続、及び会議室共同アプリケーションのために設計された。ＩｒＤＡに関する詳細は、ＩｒＤＡウェブ・サイト"http://www.irda.org"で見い出される。

【００１２】ホームＲＦ（共用無線アクセス・プロトコル（ＳＷＡＰ）にもとづく）は、装置を接続するために使用され得る動作環境の別の例である。ホームＲＦワーキング・グループは、家庭内または周辺のＰＣと、家電製品との間の無線デジタル通信のための開かれた業界仕様を確立することにより、広範囲に渡る相互運用可能な消費者製品のための基礎を提供するために結成された。ワーキング・グループには、パーソナル・コンピュータ、家電製品、周辺装置、通信、ソフトウェア、及び半導体業界からの主要企業が含まれ、ＳＷＡＰと呼ばれる家庭における無線通信のための仕様を開発中である。ホームＲＦ　ＳＷＡＰシステムは、音声及びデータ・トラフィックの両方を伝送し、公衆交換電話網（ＰＳＴＮ）及びインターネットと相互運用するように設計される。すなわち、これは２４００ＭＨｚボーで動作し、デジタル周波ホッピング・スプレッド・スペクトル無線を使用する。ＳＷＡＰ技術は既存のコードレス電話（ＤＥＣＴ）及び無線ＬＡＮ技術の拡張から導出され、ホーム・コードレス・サービスの新たなクラスを可能にする。これは対話音声及び他の時間に厳格なサービスの転送を提供する時分割多重アクセス（ＴＤＭＡ）サービスと、高速パケット・データの転送のためのキャリア検知多重アクセス／衝突回避（ＣＤＭＡ／ＣＡ）サービスの両方をサポートする。ＳＷＡＰシステムはアドホックネットワークとして、または接続ポイントの制御に従う管理ネットワークとして動作する。アドホックネットワークでは、データ通信だけがサポートされ、全てのステーションが等しく、ネットワークの制御がステーション間で分散される。対話音声などの時間に厳格な通信では、ＰＳＴＮへのゲートウェイを提供する接続ポイントが、システムを調整するために要求される。ステーションはＣＳＭＡ／ＣＡを使用し、接続ポイント及び他のステーションと通信する。ホームＲＦに関する詳細は、ホーム無線周波ワーキング・グループのウェブ・サイト"http://www.homerf.org"で見い出される。ＳＷＡＰ仕様１．０が参考として本明細書に組み込まれる。

【００１３】伝送される情報は、意図された受信者に制限され、誰にでも好適な訳ではない。秘密の及び認証された通信を想定すると、暗号化方式が役に立ち、有用である。暗号化システムは、メッセージが"秘密（secure）"となるように、メッセージを送信者から受信者に媒体を介して送信するためのシステムである。すなわち、意図された受信者だけがメッセージを復元することができる。暗号化システムは平文とも呼ばれるメッセージを、暗号文と呼ばれる暗号化形式に変換する。暗号化は、暗号キーを用いてメッセージを操作または変換することにより達成される。受信者は暗号文を平文に逆変換することにより、メッセージを解読する。これは暗号キーを用いて、操作または変換プロセスを逆処理することにより実行される。こうした暗号化伝送は、送信者及び受信者だけが暗号キーの知識を有する限り、安全である。過去に、公開キー暗号化システムなどの幾つかの暗号化システムが提案されている。公開キー暗号化システムでは、私用キーが常に算術的に公開キーにリンクされる。例えば、既知の公開キー暗号化システムは、Diffie-Hellmanキー規約、ＲＳＡ方式、またはＥＩＧａｍａｌ方式である。適応選択された暗号文攻撃に対して多分安全であろう順応性の無い公開キー暗号化システムが、R. Cramer及びV. Shoupにより提案されている。

【００１４】

【発明が解決しようとする課題】本発明の目的は、ネットワーク化普及環境における装置間の情報交換のための技法を提供することである。

【００１５】本発明の別の目的は、通信ピアを識別する技法を提供することである。

【００１６】更に本発明の別の目的は、少なくとも２つの装置間で、認証された通信セッションを確立するための技法を提供することである。

【００１７】更に本発明の別の目的は、少なくとも２つの装置間での、プライバシを保証する秘密の通信セッションのための技法を提供することである。

【００１８】

【課題を解決するための手段】本発明は一般にローカル・ネットワークに関し、特に、認証されたまたは秘密の通信セッションのセットアップに関する。局所的に分散された装置がセッションを確立し、情報を交換することを可能にする初期技法が提案される。こうしたセッションは、機能ユニットまたは装置間のデータ通信の目的で使用される。ここで用語"セッション"は、接続の確立、保守、及び解除の間に発生する全ての活動を意味する。本発明によれば、ネットワーク化普及コンピュータ環境において、少なくとも２つの装置がセッションに参加する。

【００１９】基本概念は、ユーザが着用するパーソナル・アシスタントなどの個人用装置である第１の装置と、ユーザの近くにあるサーバ装置などの第２の装置との間で、認証されたセッション、すなわちユーザにより許可されたセッションを確立したいユーザが、有向短距離通信リンクを使用し、通信セッションを開始する。従って、第１の装置が暗号化情報及び通信パラメータをタ－

ゲット装置に伝送する。ターゲット装置すなわち第２の装置は、受信情報及びパラメータを使用し、発信装置すなわち第１の装置への無線同報接続を確立する。本発明の別の部分は、秘密セッションを保証するキーの実装、及び個人用装置とサーバ装置間の通信が発生する時間フレームの制御である。

【００２０】ユーザの個人用装置とサーバ装置、例えば銀行端末との間で認証されたセッションを確立するために、ユーザは個人用装置によりサーバ装置を指し示すか、少なくともこの方向を指定し、例えば赤外線チャネルなどの単方向無線通信チャネルを介して、パスワード、公開キー、セッション・キー、識別パラメータ、及び通信パラメータなどを含むシーケンスまたは初期シーケンスを伝送する。シーケンスの受信後、サーバ装置は無線同報媒体を介して、暗号化情報を返送することにより応答する。暗号化情報は、個人用装置によってのみ解読され、使用され得る。この応答は、無線同報媒体を介する以後の通信のためのサーバ装置からの情報、キー、セッション・キー、及び通信パラメータを含み得る。個人用装置が暗号化情報を受信する。

【００２１】無線同報媒体を介する秘密セッションのために、キーが交換される。従って、無線同報媒体を介する暗号化通信が発生する。

【００２２】どの装置が通信パラメータまたはセッション・キーを送信するかは、問題でない。

【００２３】それにも関わらず、個人用装置をサーバ装置の方向に配置する要求は、通信パートナを選択するための非常に直覚的な方法を許容する。人々は子供の時から物を指し示すことになれている。更に、指し示す方法は、明示的に通信ターゲットを選択する利点を有する。すなわち、例えばＰＡＮリンクでは、ユーザは実際に通信ターゲットに触れる必要があり、レーザ・リンクでは、通信パートナが視覚的に選択され得る。

【００２４】２つの装置が同一の無線同報媒体を共用し、ローカル・ネットワークの一部の場合、たとえ個人用装置を有するユーザが別の部屋または階に歩いていくことにより、自分の位置を変えても、開始セッションが継続され得る利点がある。これは個人用装置が大きなファイルをダウンロードしたり、サーバ装置と長い時間通信する場合に役立つ。無線同報媒体としては、赤外線（ＩＲ）チャネルまたは無線周波（ＲＦ）チャネル、特にＩｒＤＡチャネル、ホームＲＦチャネル、ブルートゥース・チャネル、パーソナル・エリア・ネットワーク（ＰＡＮ）・チャネル、音響チャネル、またはユーザに広範囲のアクションを保証する他のチャネルが使用され得る。

【００２５】通信セッションを開始し、機密情報を含み得る初期シーケンスを伝送するために、単方向無線通信チャネルがターゲット装置だけが初期シーケンスを受信することを保証する。これは特に、有向チャネルが視線リンクとして使用され得る場合に有利である。なぜなら、他の当事者が立ち聞きし、初期シーケンスを受信できないからである。こうしたチャネルは、赤外線またはレーザ・チャネルなどの光チャネル、パーソナル・エリア・ネットワーク（ＰＡＮ）・チャネル、有向無線周波（ＲＦ）チャネル、誘導チャネル、容量チャネル、または短距離有向通信リンクに好適な他のチャネルである。

【００２６】サーバ装置が個人用装置からのシーケンスの受信を知らせる場合、ユーザはフィードバックを獲得し、サーバ装置が追加の通信のために準備完了状態であることを知る利点がある。これはランプ、ＬＥＤまたはラウドスピーカにより与えられる光信号または音響信号により示される。

【００２７】サーバ装置が周期的に個人装置からのシーケンスに傾聴するとき、送信されるシーケンスが即時処理され得る利点がある。

【００２８】個人装置が例えばＰＡＮによりユーザに接続される場合、通信をセットアップすることは非常に単純である。なぜなら、ユーザは直覚的にサーバ装置に触れ、自身の人体を介して有向無線通信チャネルを開始するからである。認証されたセッションをセットアップするために、追加のカードや他の物は必要とされない。

【００２９】無線同報媒体を介する応答及び追加の通信が、暗号化システムの使用により保護される場合、交換情報が完全に隠され、別の誰かにより暴露され得ない利点がある。好適なシステムは、公開キーが１度交換される公開キー暗号化システムである。

【００３０】更に本発明の別の利点は、無線単方向リンクの場合、個人装置とサーバ装置との直接的な接触が必要でないことである。例えば、キャッシュカード、スマートカード、または個人装置内の任意の他のカード、或いは個人装置自体に、例えば電子メール、データまたは金額などの情報が、相対距離からロードまたはアップロードされ得る。カードは装置または読取り装置内に配置される必要はなく、このことは読出しエラーを回避し、ＰＩＮコードを余分に形成し、時間の節約に役立つ。

【００３１】秘密セッションがサーバ装置のすぐそばまたは正面で開始し、遠い距離において安全に継続され得る。サーバ装置はこれらの装置が有用な至る所、例えば銀行、オフィス、倉庫、ショッピング・センタ及び屋外などに設置される。これはユーザに行動の大きな独立性及び自由をもたらす。例えば、サーバ装置がコンサートの広告のすぐ近くに配置される。このコンサートのチケットは、ユーザが駅のプラットフォームで電車を待っている間に、コンサートの広告を見るときに購入され、代金を支払われる。チケットはカード上または個人用装置上に電子的に記憶されるか、コンサートの入口においてアップロードされ得る。ユーザはチケット売場で行列になって待つ必要はなく、チケットを買い忘れることもない。

【００３２】
【発明の実施の形態】本発明の目的上、用語"ネットワーク化普及コンピュータ環境（networked pervasive computing environment）"は、無線ネットワーキング技術を通じて通信する携帯用情報装置及び固定情報装置の両方の環境として定義される。こうした環境内での装置間の通信は、近距離を基本とする。これらの装置の始動通信範囲は小さい。従って、装置が近い距離にあるときだけ、セッションが開始され得る。更に、通信関係の確立は、アドホック的性質（ad-hoc nature）を有する。これはすなわち、物理層上での通信が、任意の２つの装置が近い距離にあるとき、常に発生し得ることを意味する。こうした装置のユーザは情報の流れを制御する必要があり、これは特に、クレジットカード詳細や権限などの機密情報に当てはまる。種々の問題は、機構について述べるセッション制御である。
【００３３】本発明の状況では、ローカル・ネットワークが、互いの相互通信範囲内の少なくとも２つの装置からなるネットワークとして定義される。こうしたローカル・ネットワーク内では、装置は配線式ネットワークの必要無しに、互いに通信する。ローカル・ネットワークは固定ネットワークとの接続のために、アクセス・ポイントを有する必要がない。ローカル・ネットワークは他のネットワークから完全に分離されるか、無線装置に配線式ネットワークとの接続を提供する１つ以上のアクセス・ポイントを含み得る。
【００３４】本発明に従いローカル・ネットワークを構成する特定の範囲は、実際の実装詳細に依存する。一般に、ローカル・ネットワークは、数平方メートル乃至数百平方メートルの通達範囲を有するものとして述べられる。特定の状況下では、通信範囲は更に広がる。
【００３５】本発明のネットワーキング技法は、倉庫、製造フロア、オフィス、立合場、自宅、自動車及びトラック、航空機、及び屋外などで使用され得る。
【００３６】用語"装置"は、ローカル・ネットソークのメンバである任意の種類の装置を意味する。こうした装置の例には、ラップトップ・コンピュータ、ソークパッド、ノートパッド、パーソナル・デジタル・アシスタント（ＰＤＡ）、ノートブック・コンピュータ及び他の着用可能なコンピュータ、デスクトップ・コンピュータ、コンピュータ端末、ネットワーク・コンピュータ、インターネット端末及び他のコンピュータ・システム、セットトップ・ボックス、キャッシュ・レジスタ、バーコード・スキャナ、ポイント・オブ・セールス（ＰＯＳ）端末、キオスク・システム、セルラ電話、ページャ、腕時計、デジタル時計、バッジ、スマートカード、及び他のハンドヘルド及び組み込み装置などがある。他の装置には、ヘッドセット、ヒューマン・インタフェース装置（ＨＩＤ）準拠の周辺装置、データ及び音声アクセス・ポイント、カメラ、プリンタ、ファックス・マシン、キーボード、ジョイスティック、台所器具、道具、発煙及び発火検出器などのセンサ、及び事実上あらゆる他のデジタル装置が含まれる。
【００３７】本発明と共に使用され得る着用可能なコンピュータの他の例には、"スマート・ウォレット"・コンピュータ、宝石類、または衣類など、コンピュータ風のハードウェアを装備された身の回り品がある。"スマート・ウォレット"・コンピュータに加え、着用可能なコンピュータの多数の他の変形が存在する。"ベルト"・コンピュータは、ユーザが動き回る間に、文書をサーフし（surf）、書き留め、編集することを可能にする変形である。更に別の例は、小学生用のパーソナル・デジタル・アシスタントに匹敵する子供のコンピュータである。子供のコンピュータは宿題を保持し、計算を実行し、子供が宿題を管理することを手助けする。それは他の子供のコンピュータとインタフェースし、共同作業を容易にし、また先生のコンピュータにアクセスして、宿題またはフィードバックをダウンロードする。任意の着用可能または携帯可能な装置、オフィス・ツールまたは装置、家庭用ツールまたは装置、乗り物用システム、或いは公衆用システム（自動販売機、チケット自動販売機、自動預金支払機など）が、本発明の状況において使用され得る。
【００３８】ネットワーク・トポロジ：本技法は、ポイント間及びポイント―マルチポイント間接続を有するローカル・ネットワークで使用され得る。幾つかのネットワーク・セグメント（グループ）が確立され、アドホックに一緒にリンクされ得る。ネットワーク・トポロジは、本発明のテーマよりも低レベルである。ネットワーク・トポロジの態様は、必要な程度だけ示される。本発明はネットワーク・トポロジとは無関係であり、同報を可能にする任意の種類のネットワーク・トポロジ上で使用され得る。
【００３９】ネットワーク技術：本技法は、ＲＦ、ＩＲまたは他の光技術、人体ネットワーク（ＰＡＮなど）などの、任意の無線通信技術に関連して使用され得る。
【００４０】以下では、本技法の典型的な実装（第１の実施例）について、図１及び図２に関連して述べることにする。
【００４１】図１では、ユーザの手の中にある第１の装置１と、ユーザの近くにある第２の装置２との間の情報の交換のために、認証されたセッション８をセットアップしたいユーザ７を示す簡単な概略図である。そのために、ユーザ７は第１の装置１を物理的に第２の装置２の方向に向け、接続を開始する。第１の装置１は暗号化情報を有するシーケンス５を、単方向無線通信チャネル３を介してターゲット装置すなわち第２の装置２に送信する。単方向無線通信チャネル３がセキュリティを保証する有向視線リンクとして、例えば赤外線チャネルとして確立されることが有利である。なぜなら、別の誰もリン

クを傾聴できないからである。第２の装置２は、プリンタまたは別の人間の装置であり、パスワード、キー、通信パラメータ、または識別パラメータを含むシーケンス５を受信し、受信情報を用いて第１の装置に対して、所望の認証されたセッション８をセットアップする。無線同報媒体４がその目的のために使用される。

【００４２】図２は、図１のより詳細な構成を示す。第１の装置１は、初期送信機１０、第１のトランシーバ１１、及び第１の暗号化システム１５を含む。これらの全てのユニットは第１の処理ユニット１６に接続され、後者は簡略化のために図示されていない更に別のユニットに接続される。第１のトランシーバ１１は、第１の同報受信機１２及び第１の同報送信機１３を有する。他方、第２の装置２は、初期受信機２０、第２のトランシーバ２１、及び第２の暗号化システム２５を含む。第２の装置２の全てのユニットは第２の処理ユニット２６に接続され、後者は簡略化のために図示されていない、データ処理のための更に別のユニット、またはネットワークにさえも接続される。第２のトランシーバ２１は、第２の同報送信機２２及び第２の同報受信機２３を有する。更に、第２の装置２はシグナル装置３０を示し、これはここではＬＥＤである。このＬＥＤ３０は中央処理ユニット２６に接続される。２つの暗号化システム１５、２５のタスクは、情報を暗号化及び解読し、交換される情報を隠し、保護することである。

【００４３】認証を提供するために、本技法は公開キー技法を使用する。これはすなわち、第１の当事者が、私用キー及び暗号化アルゴリズムを用いて公開キーを生成し、この公開キーを第２の当事者に送信するか、公開キーを他の当事者が使用可能にする。次に、例えば第２の当事者が、受信された公開キーを用いて情報を暗号化する。暗号化された情報が、例えば無線周波（ＲＦ）チャネルなどの無線同報媒体など、不確かな媒体またはチャネルを介して返送される。しかしながら、第１の当事者だけが私用キーを用いて、この情報を解読できる。

【００４４】本発明に従う初期技法は、次のように作用する。図２では簡略化のため示されていないユーザ７が、初期送信機１０を用いて、第１の装置１から単方向無線通信チャネル３を介してシーケンス５を送信する。ここではシーケンス５は開始トークンT_{imt}を含み、単方向無線通信チャネル３は、第２の装置２への有向ＩＲチャネルである。開始トークンT_{imt}は、第１の装置１の公開キーK^{P}_{pub}、及びランダムに選択されたアドホックデータ$nonce_P$を含む。単方向無線通信チャネル３を介して、開始トークンT_{imt}を伝送することにより、目標の第２の装置２だけがそれを受信し、応答することができる。第２の装置２が初期受信機２０においてシーケンス５を受信し、第２の処理ユニット２６がシーケンス５を通知され、受け渡される場合、ＬＥＤ３０が第１の中央処理ユニット１６によりトリガされ、ユーザ７に第２の装置２が準備完了状態で、通信セッションを開始できることを知らせる。セッションはいつでもユーザにより制御され、これはすなわち、ユーザが即時セッションを停止できることを意味する。通常、第２の装置２は、受信される開始トークンT_{imt}に応答して、第２の同報送信機２２から無線同報媒体４を介して、公開キー・トークンT_{pub}を応答６として第１の装置１に返送する。ここでは無線同報媒体４は無線周波（ＲＦ）である。第２の暗号化システム２５により生成される公開キー・トークンT_{pub}は、第２の装置２の公開キーK^{S}_{pub}、及び受信されたアドホックデータ$nonce_P$の連結を含む。公開キー・トークンT_{pub}は、開始トークンT_{imt}内で受信された第１の装置の公開キーK^{P}_{pub}を用いて暗号化される。最後に、第１の装置１は第１の主受信機１２により応答を受信し、第１の処理ユニット１６及び第１の暗号化システム１５により、この応答を処理し、第１の同報送信機１３により、通信パラメータ・トークンT_{com}を含む通信シーケンス９を返送する。この通信シーケンス９もまた、無線同報媒体４を介して伝送され、第２の装置２の第２の同報受信機２３により受信される。通信パラメータ・トークンT_{com}は、第２の装置２の受信公開キーK^{S}_{pub}により暗号化される。

【００４５】交換されるトークンは、算術的に次のように表すことができる。

【数１】$T_{imt} = K^{F}_{pub} || nonce_P$

【数２】$T_{pub} = [K^{S}_{pub} || nonce_P] K^{P}_{pub}$

【数３】$T_{com} = [Com] K^{S}_{pub}$

【００４６】第１の暗号化システム１５は、開始トークンT_{init}及び通信パラメータ・トークンT_{com}を提供し、第２の暗号化システムは公開キー・トークンT_{pub}を提供する。

【００４７】第１の装置と第２の装置間の続く通信は、第１のトランシーバ１１及び第２のトランシーバ２１を用い、無線同報媒体４を介して発生する。それにより、第１の装置１により指定された通信パラメータが使用される。

【００４８】セッションの認証について、前述の第１の実施例で述べた。しかしながら、クレジットカード情報などの機密情報を交換するために、認証だけでは十分でない。第１の装置と第２の装置間の保護された専用通信リンクが必要とされる。従って、第２の実施例は、通信パラメータ・トークンT_{com}内に、第１の装置１の第１の暗号化システム１４により生成される暗号化セッション・キーK^{F}_{sess}を含むことにより達成される。両方の装置間の続く各通信は、このセッション・キーK^{P}_{sess}を用いて暗号化される。

【００４９】別の実施例が、第１及び第２の実施例に関連して、以下で述べられる。一般に、個人用装置である第１の装置１と、サーバ装置である第２の装置との間の対話は、特定のタイミング状況において発生する。サー

バ装置２が開始トークンT_{init}を何度も再使用することを阻止するために、満期日T_{b}^{init}が開始トークンT_{init}に付加される。両者はシーケンス５内で伝送される。個人用装置１は、開始トークンT_{init}に付加された満期日T_{b}^{init}がまだ過ぎていなければ、公開キー・トークンT_{pub}に応答する。満期日T_{b}^{init}は個人用装置１の時間の観念に関連する。

【００５０】更に別の実施例は、前述の実施例の変形である。満期日開始トークンT_{b}^{init}同様、満期日T_{b}^{sess}が、個人装置または第１の装置１により生成されるセッション・キーK_{sess}^{p}に付加され、無線同報媒体４を介して伝送される。満期日T_{b}^{sess}の実装は、応答装置２に応答の定義期限を提供する。この期限が過ぎると、伝送は要求されず、セッションは停止される。これは携帯装置の電力を節約し、セキュリティを提供するために役立つ。

【００５１】開始トークンT_{init}を有するシーケンス５を、無線通信チャネル３を介してサーバ装置２に転送することは、ユーザ７の明示的な制御に従うべきである。単方向無線通信チャネル３として使用される技術に応じて、この問題は異なって扱われる。単方向無線通信チャネル３（以下、（短距離）単方向チャネル）を介する通信は、デフォルト指定により無効にされる。単方向チャネル３がレーザ・ポインタの光リンクの場合、次の２段階プロシージャが問題を解決する。すなわち、（１）ユーザ７が第１のボタンを押下して、レーザを活動化し、レーザビームが目標対象物の表面に当たるとき、レーザビーム・スポットのビジュアル制御により、レーザを所望の方向に向け、（２）ユーザ７がレーザビームが対象物に当たっていると判断するとき、ユーザは第２のボタンを押下し、実際に開始トークンT_{init}を有するシーケンス５をターゲット装置２に送信する。単方向チャネル３がＰＡＮ技術にもとづく場合、次の２段階プロシージャが問題を解決する。すなわち、（１）ユーザ７が第１のボタンを押下することにより、単方向チャネル３を使用可能にする。一旦活動化されると、単方向チャネル３はある限定時間δｔの間活動化され、その間に、ユーザ７はＰＡＮ可能面に触れることにより、シーケンス５を有向チャネル３を介して伝送する機会を有する。（２）ユーザ７はＰＡＮ可能面に触れることにより、実際にシーケンス５を単方向チャネルを介して伝送する。δＴの経過後、単方向チャネル３を介する通信が即時無効化され、追加の偶発的な情報交換を阻止する。

【００５２】活動化プロシージャの拡張は、ユーザが個人用装置の第１のボタンを繰り返し押下することにより、δＴを長引かせることができる場合である。

【００５３】更に、個人用装置は、汎用無線通信チャネル３を即時無効化するための類似の手段を提供すべきである。

【００５４】任意の開示実施例が、ここで示された１つのまたは複数の他の実施例と組み合わされ得る。これは実施例の１つ以上のフィーチャについても可能である。

【００５５】まとめとして、本発明の構成に関して以下の事項を開示する。

【００５６】（１）第１の装置と少なくとも第２のリモート装置との間の情報交換のための方法であって、前記第１の装置と前記第２のリモート装置との間の単方向無線通信チャネルを始動するステップと、前記単方向無線通信チャネルを介して、前記第１の装置から前記第２のリモート装置にシーケンスを送信し、前記第２のリモート装置に暗号化情報を提供するステップと、前記暗号化情報を暗号化のために使用し、無線同報媒体を介して、前記第１の装置に暗号化応答を送信するステップとを含む、方法。

（２）前記２つの装置が前記無線同報媒体を共用し、ローカル・ネットワークの一部である、前記（１）記載の方法。

（３）前記単方向無線通信チャネルが光チャネル、パーソナル・エリア・ネットワーク（ＰＡＮ）・チャネル、有向無線周波チャネル、誘導性チャネル、または容量性チャネルである、前記（１）記載の方法。

（４）前記単方向無線通信チャネルが有向チャネルである、前記（１）または（３）記載の方法。

（５）前記有向単方向無線通信チャネルが視線リンクである、前記（４）記載の方法。

（６）前記第１の装置の初期送信機が、前記単方向無線通信チャネルが前記第２の装置に向けられるように配置される、前記（１）記載の方法。

（７）前記無線同報媒体が光チャネル、音響チャネル、無線周波（ＲＦ）チャネル、ホームＲＦチャネル、ブルートゥース・チャネル、またはパーソナル・エリア・ネットワーク（ＰＡＮ）・チャネルである、前記（１）または（２）記載の方法。

（８）前記単方向無線通信チャネルが数メートルの通達距離を有し、前記無線同報媒体のチャネルが、前記単方向無線通信チャネルの前記通達距離と同一の、またはそれ以上の通達距離を有する、前記（１）記載の方法。

（９）前記第２のリモート装置が前記シーケンスを受信する、前記（１）記載の方法。

（１０）前記第２のリモート装置が前記第１の装置からの前記シーケンスの受信を、光または音響信号により知らせる、前記（１）記載の方法。

（１１）前記第２のリモート装置が前記シーケンスを周期的に傾聴する、前記（１）記載の方法。

（１２）前記第１の装置がユーザに接続され、前記ユーザが前記第２のリモート装置に触れることにより、該ユーザの人体を介して前記単方向無線通信チャネルを始動する、前記（１）記載の方法。

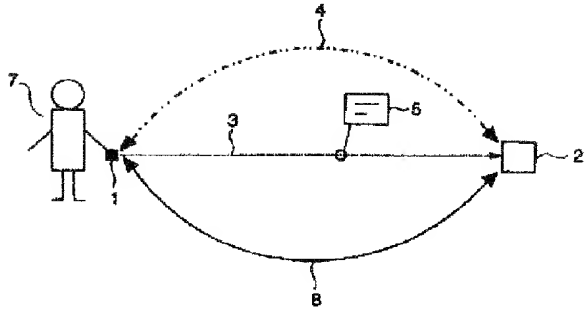
（１３）前記２つの装置の１つが、少なくとも通信パラメータまたはセッション・キーを送信する、前記（１）

記載の方法。
（１４）前記無線同報媒体を介する前記応答が、公開キー暗号化システムを含む、暗号化システムにより保護される、前記（１）記載の方法。
（１５）前記暗号化情報がパスワードまたは公開キーを含む、前記（１）記載の方法。
（１６）少なくとも１つのリモート装置との情報交換のための装置であって、単方向無線通信チャネルを介して、前記リモート装置にシーケンスを送信する初期送信機と、前記リモート装置から無線同報媒体を介して暗号化情報を受信する受信機と、前記単方向無線通信チャネルを介して前記リモート装置に送信可能な暗号化情報を提供する暗号化システムとを含み、前記受信機が前記無線同報媒体を介して、前記暗号化システムにより処理可能な暗号化情報を受信する、装置。
（１７）少なくとも１つの装置との情報交換のための装置であって、単方向無線通信チャネルを介して、前記装置からシーケンスを受信し、暗号化情報を獲得する初期受信機と、前記暗号化情報を処理する暗号化システムと、暗号化情報を無線同報媒体を介して前記装置に送信する送信機とを含む、装置。
（１８）情報を符号化及び復号する暗号化システムを有する第１の装置及び第２の装置を含む、情報の交換のための通信システムであって、前記第１の装置が、単方向無線通信チャネルを介して、前記第２の装置にシーケンスを送信し、前記第２の装置に暗号化情報を提供する初期送信機と、無線同報媒体を介する前記第１及び第２の装置間の暗号化通信のための第１のトランシーバとを含み、前記第２の装置が、前記単方向無線通信チャネルを介して、前記第１の装置から前記シーケンスを受信し、前記暗号化情報を獲得する初期受信機と、前記無線同報媒体を介する前記第１及び第２の装置間の暗号化通信のための第２のトランシーバとを含む、通信システム。
（１９）前記無線同報媒体を介して暗号化情報を送信可能な送信機を含む、前記（１６）記載の装置。
（２０）前記初期送信機が前記シーケンスを前記単方向無線通信チャネルを介して、数メートルの通達距離内で送信する、前記（１６）記載の装置。
（２１）前記無線同報媒体が光チャネル、音響チャネル、無線周波（ＲＦ）チャネル、ホームＲＦチャネル、ブルートゥース・チャネル、またはパーソナル・エリア・ネットワーク（ＰＡＮ）・チャネルである、前記（１６）または（１７）記載の装置。
（２２）前記無線同報媒体が前記単方向無線通信チャネルの通達距離と同一の、またはそれ以上の通達距離を有する、前記（１６）または（１７）記載の装置。
（２３）ＬＥＤなどの光装置またはラウドスピーカなどの音響装置により、前記シーケンスの受信を知らせるシグナル装置を含む、前記（１７）記載の装置。
（２４）前記初期受信機が前記シーケンスを周期的に傾聴する、前記（１７）記載の装置。
（２５）前記２つの装置の１つが通信パラメータ及びセッション・キーを送信できる、前記（１８）記載の通信システム。
（２６）前記２つの装置が前記無線同報媒体を共用し、ローカル・ネットワークの一部である、前記（１８）記載の通信システム。
（２７）前記第１の装置の前記初期送信機が、前記単方向無線通信チャネルが視線リンクにより前記第２の装置に向けられるように配置される、前記（１８）記載の通信システム。

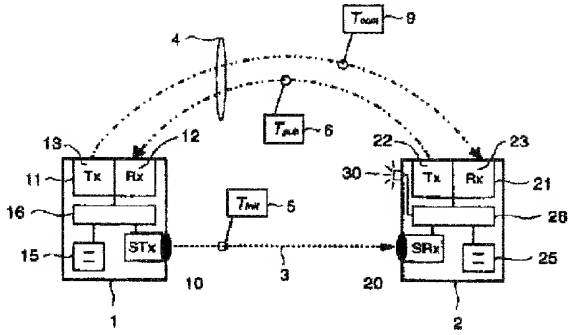
【図面の簡単な説明】
【図１】ユーザが自身の個人用装置とリモート・サーバ装置との間で、認証されたセッションを確立したい場合に、本発明に従うアプリケーションの概略図である。
【図２】図１の詳細概略図である。

【符号の説明】
１　第１の装置
２　第２の装置
３　単方向無線通信チャネル
４　無線同報媒体
５、９　通信シーケンス
７　ユーザ
８　認証されたセッション
９　応答
１０　初期送信機
１１、２１　トランシーバ
１２、２３　同報受信機
１３、２２　同報送信機
１５、２５　暗号化システム
１６、２６　処理ユニット
２０　初期受信機
３０　ＬＥＤ

【図１】



【図２】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
		Ｈ０４Ｌ　11/00	３１０Ｂ

(72)発明者　ダーク・フセマン
スイス、シィ・エイチ－8134　アドリスウィル、クレブスバックウェグ　4